TIA and The Protection of Personal Information Act (POPIA) White Paper

February 20, 2018 – note that content is subject to change

TIA Technology
The Workplace,
140a Kelvin drive,
Morningside manor,
Johannesburg,
South Africa
T +27 11 064 1677
W tiatechnology.com
E iwi@tiatechnology.com

Contents

Introduction

Personal information is protected as a right to privacy in the Constitution for South Africa. The introduction of the Protection of Personal Information Act (POPIA) in 2013 supports a dedicated legislation to protect our personal information. The Act regulates how companies handle data and introduces a regulatory body to monitor and enforce protection of personal information.

The POPI Act is not yet in force and the effective date is not yet known. The Information Regulator has been established and it is expected that a presidential announcement of effective date will be made in early 2018. Companies will have one year from the effective date to comply.

The Act provides people with more control and transparency over their personal information and better protection of privacy. The impact of POPIA is organisation-wide and will impact all processes, systems and roles, including solutions that store personal information, such as the TIA Solution.

This white paper briefly outlines the key requirements in the regulation and discusses how the requirements will be implemented and supported by the TIA POPIA Compliance Package. The package is a combination of amendments to the TIA Solution, including configuration and implementation updates, as well as advice on roadmap and handling of data in associated solutions. The package functionality is introduced with TIA 7.5.1 and TIA 6.4.4. and is implemented by TIA Services & Solutions, who will:

- Present a plan for custom implementation
- Ensure that any customised information, for example, captured in flex fields, are included in scope
- Install the solution at the customer site and work with onsite QA to validate the updated solution

All companies with domicile within South Africa must comply with POPIA. Failure to do so may result in heavy fines, up to R10 million, damage to reputation and loss of customers. Severe cases can result in imprisonment.

Need more information?

TIA White Papers – TIA Technology has created several industry-relevant white papers that can be downloaded from: www.tiatechnology.com

You are always welcome to contact TIA Technology at iwi@tiatechnology.com.

Regulation requirements

POPIA describes how personal information is to be treated and how and whom should be held accountable for controlling that the rules are followed. This section provides an overview of the rules that need to be followed to meet compliance:

POPIA dictates the following eight conditions for compliance:

1. **Accountability** – Insurance companies are to ensure lawful handling and processing of personal information.
2. **Processing limitations** – Personal information can only be processed for lawful proposes[1] and only with consent from the affected person. Consent may be withdrawn and the halt of information processing may be requested.
3. **Purpose specification** – Personal information can only be collected and stored for a specific and well-defined purpose, and only based on consent. Anonymised information is to be deleted as soon as reasonably and practically possible after no purpose exists.
4. **Further processing limitations** – Personal information may not be processed for a secondary purpose unless that processing is compatible with the original purpose.
5. **Information dissemination and quality** – Companies are to ensure that personal information is complete, accurate, not misleading and updated.
6. **Openness** – Companies collecting personal information must ensure the affected person is informed that the information has been collected and why.
7. **Security safeguards** – Personal information must be kept secure against the risk of loss, unauthorised access, interference, modification, destruction, and disclosure.
8. **Data subject participation** – It must be possible to request information as to where one's own personal information is held, and it must be possible to get involved in the correction and/or deletion of any personal information.

References

The below sources were cited to create this document.

• The Information Regulator	Independent organisation established based on POPI
• The POPI Act	The Act published in 2013

[1] to fulfill a contract, protect the data subject, to comply with law

TIA Solution and The POPI Act

This chapter will describe TIA's support for all eight conditions in the act. Please note, not all eight conditions have a direct impact on core applications.

- Condition 1: **Accountability** ensures that the responsibility for following the Act is placed with the insurers. This condition has no direct impact on a TIA Solution installation.
- Condition 2: **Processing limitations** addresses consent and collection of information for a purpose, which has no direct impact on existing TIA Solution implementations. However, the Act dictates that processing of information is to be stopped if the data subject objects. Please find a description of the functionality under "Consent and suspension of information handling ".
- Condition 3: **Purpose specification** will have an impact on a TIA Solution implementation as the condition describes what can be stored and under which conditions information can kept. The POPIA Compliance Package includes a rule based data deletion concept to support compliance to this condition. See details under "Deletion of personal information".
- Condition 4: **Further processing limitations** describes that the processing of information should be compatible with the original purpose. The TIA Solution only processes information for insurance. Hence, the condition will not have a direct impact on TIA Solution installations.
- Condition 5: **Information quality** describes that information is to be kept updated, which is mostly relevant for internal processes and interfaces. TIA Solution installations allow for the update of information and keep audits of the changes.
- Condition 6: **Openness** has no direct impact on a TIA Solution implementation as it describes the level of information that is to be provided to the customers/data subject and that all processes are to be documented. Internal processes are documented outside the TIA Solution and will include a broader view than TIA alone processes. TIA supports the work of the documentation process via TIA process descriptions in TIAWIKI.
- Condition 7: **Security safeguards** states that the integrity and confidentiality of information must be secured through appropriate organisational and technical measures. The measures are industry specific. The existing authorisation system ensures that unauthorised deletion or access to information of personal information is prohibited. See more details under "Access limitation".

  This section also discusses additional security for "special personal information". Insurers must notify customers and authorities in case of a security breach. The TIA POPIA Compliance Package introduces additional audits for viewing personal information to ensure compliance.
- Condition 8: **Data subject participation** ensures that everybody can request insight into their own stored personal information and request updates/deletion of information if outdated. TIA data deletion (see "Deletion of personal information") ensures that information is deleted when eligible for deletion and not before. However, an authorised Information Officer can force a deletion. The TIA POPIA Compliance Package introduces new integration possibilities for exposing personal information to the insured (See "Self-service for customer participation"). It is suggested that customer self-

service is considered for information updates, which can be achieved via TIA web services (REST or SOAP dependent on TIA version).

These requirements and the way they are handled in TIA are discussed below. The described solutions are based on new compliant-specific features introduced to the TIA solution in TIA 7.5.1 and TIA 6.4.4. The right to use the new functionality is obtained through a separate contract with TIA Technology.

Consent and suspension of information handling

During a typical workday, insurers collect information. POPIA requires that information is collected and stored with a purpose and in consent with the data subject (the insured).

TIA stores information but does not collect the information directly. Data feeds will always be done via an interface. The POPI Act will therefore not directly impact TIA data.

Consent can be stored in TIA without upgrades of the existing TIA installation. A "consent received" can be marked on the name or policy record[2]. Physically signed consent documents can be stored as attachments with the TIA case module and indexed to a specific customer and/or policy.

The insurer can withdraw the consent for data handling, for example, in situations when a dispute exits between the parties regarding the insurer's right to process the individual's information. In this case, manual data processing can be suspended.

TIA's new compliant features enable insurers to manage temporary suspension using an option on the party object. When enabled, all data related to the party are in "read-only" mode and no data can be changed by a user. Underlying processes continue and premium is still collected. (See next section for cases where the insured has left the company and has withdrawn consent.)

Deletion of personal information

Personal information collected lawfully and with the insured's consent are stored for a variety of reasons. Information can be retained if the information is needed to serve the original purpose. Insurers are obliged to destroy, delete or de-identify records when storing of the information does not serve the original purpose.

The TIA POPIA Compliance Package includes functionality that ensures all personal information can be cleaned up from the system when a business relationship expires. TIA's clean-up function offers "house-keeping" to ensure that data eligible for deletion based on age is removed from a production environment.

TIA POPIA Compliance Package supports these insurer needs:

[2] Utilizing TIA flex field concept

- The need to comply with regulations concerning handling of personal information. Transient information, for example, data used for quotes or for parties created on self-service websites, can typically be deleted.
- The need to periodically trim the database for obsolete data; removing data frees up space and has a positive effect on system performance.

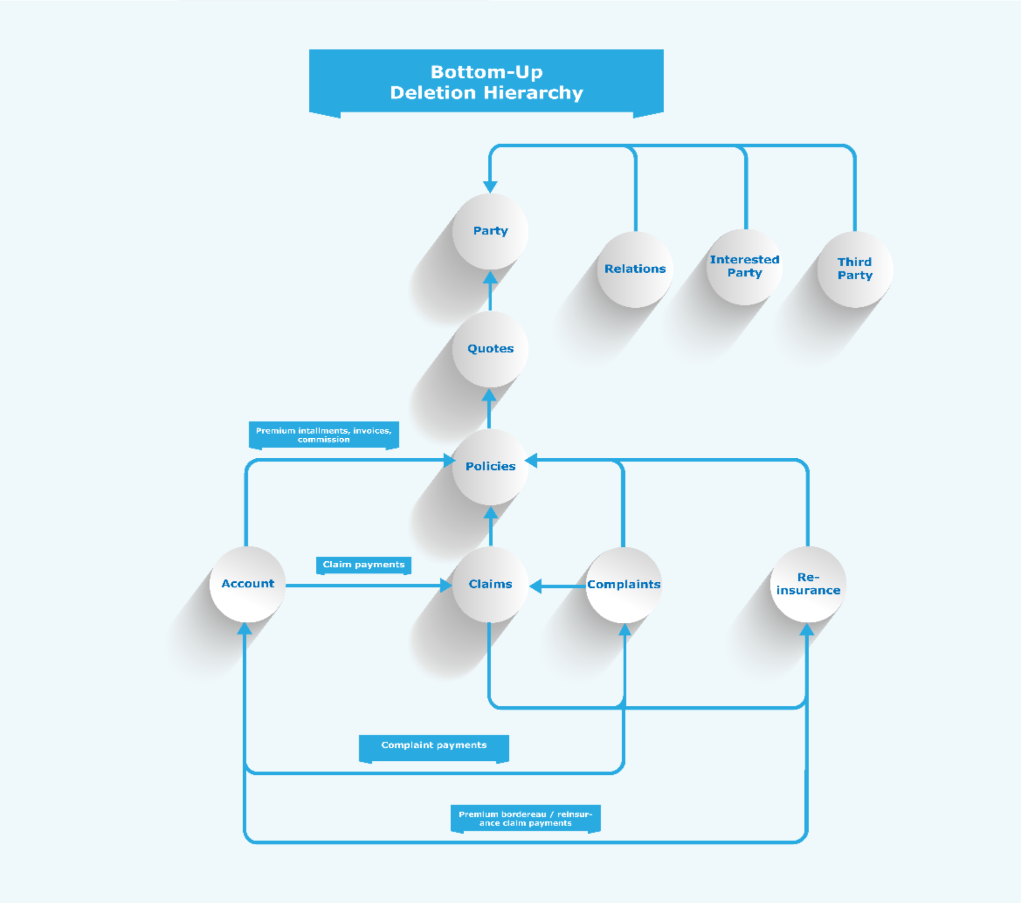
The TIA POPIA Compliance Package consists of a set of programs to clean up personal and obsolete information stored in TIA modules. Processing will be based on a set of rules that are defined and configured on site. The rules can be based on business relationships and can be set up by business users (for example, compliance officers), which makes the solution flexible and adjustable. Rules might specify that customers with no claims and no polices are deleted after 30 days, customers with personal injury claims are stored for 30 years, but policies and claims not related to the personal injury are deleted sooner.

The automated processing is supplemented with a manual option: users can delete data manually through the TIA UI by providing exact instances (party number or policy numer) to be deleted. This could, for example, be relevant in instances where existing data is found to be wrong.

The TIA POPIA Compliance Package also includes clean-up of old transactional data in single, high-volume static database tables. Configuration options ensure that the storage period is long enough to satisfy specific company needs. Manual deletions and the automated process follow the same validation rules.

Stringent system validations ensure that data integrity is maintained at all times in case of data deletion.

The diagram below illustrates functional dependencies in the main TIA modules where personal information is stored. When obsolete data is deleted, the process starts at the bottom and continues upwards.



For example, account data is deleted first, starting from the bottom. If account data is deleted successfully, then further entities, such as claims, can be processed. Policies can be erased when all related claims and financial data have been deleted. As a last step, party entity and all related information is cleaned. This mechanism ensures that qoutes (without claims and account transactions) are handled after a shorter period than policies and claims.

Access limitation

The TIA Solution already includes authorisation and access to settings that can be used to ensure that personal information can be accessed by appropriate company employees within a department. For example, it ensures that only claims handlers can access and update claims data. TIA authorisation settings enable insurers to define the users or user groups who can view and edit data.

Insurance companies should, in general, only collect and store information needed to access the risk to be insured. However, we see cases where it is relevant to collect “special personal information” such as medical history. POPIA outlines that the information may only be processed by responsible parties, subject to an obligation of confidentiality by office, employment, profession or legal provision. This has led TIA to introduce a new granular authorisation level, which enforces that only authorised groups within a department can access "special personal information", e.g., only employees working with personal injury claims can access medical history and claims information. This will require that "special personal information" is stored in the dedicated area.

The new authorisation settings control access to the following information:

- **Party information**: Data identifying a customer is not considered special, hence, no restriction is added to party data.
- **Policy related information**: Access can be limited to specific clauses and coverages for a given policy. Many person insurances hold "special personal information" on the "description of the insured object", for example a person. Consequently, TIA's role based access control is on the insured object level.
- **Financial transactions**: Payment instructions and general payment information is not to include "special personal information", hence TIA is enforcing restrictions to financial/account information.
- **Claims data and history**: TIA's authorisation mechanism controls access to specific types of claims. Handlers without authorisation can see that a claim exists but not the content; only authorised handlers can see and work on personal injury claims.
- **Communication and documents**: TIA ensures that communications and documents, including images, are subject to the rules of the related entity, for example claims or policies.

The solution supports a granular security access, as shown in an example below:

Level 1	Security level 1: All claim handlers have this level as a minimum. Allows the user to handle all standard property
Level 2	Security Level 2: Allows the user to also handle auto claims
Level 3	Security Level 3: Allows the user to also handle commercial claims
Level 4	Security Level 4: Allows the user to also handle casualty claims
Level 5	Security Level 5: Allows the user to also handle workers' compensation claims

Note that, by default, users have no access: all users need to be assigned a security level to access data.

Monitoring user activity

A breach in data security needs to be identified and needs to trigger the appropriate actions, depending on the severity.

The current TIA version reduces the risk of a breach by automatically enforcing timeout in the front-end.

Any data modification in TIA is logged with a user id and a time stamp. This makes it possible to document who changed or entered data, and an audit trail is in place in case of an incident resulting in data changes. TIA's audit mechanism also tracks unsuccessful log-in attempts.

The TIA POPIA Compliance Package enables logging of viewed data, which supports the documentation of the impact of a possible breach. The package provides relevant context information (including IP-address) for Oracle Audit. Oracle Audit can be activated for logging of user activities. TIA provides guidelines and sample configuration tracking to follow the session and helps identify compromising actions and who has been compromised.

Self-Service for customer participation

The TIA POPIA Compliance Package supports requirements for access to personal information and the right for correct data with one standard solution. The philosophy is to provide a dynamic output Application Programming Interface (API) and implementation guidelines, which will enable and speed up the introduction of customer facing communication like portal sites or standard documents.

The new dynamic output API solution enables insurance companies to configure an unlimited number of RESTful APIs that will return a response in JSON format to be used in preferred communication channels with customers, for example, in customer portals, output solutions, etc.

The existing APIs will support the right to request updates to personal information. TIA provides a standard API for updating information. The format depends on the TIA version.

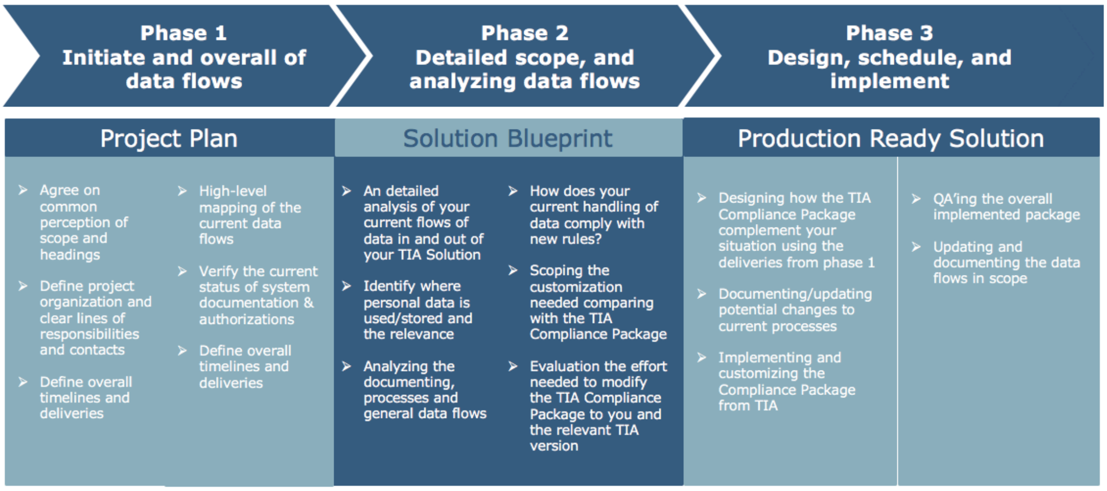
The flexible solution offers the freedom to insurance companies to interpret for themselves which personal information the customers have the right to access. TIA will provide examples for inspiration. The solution will support variations in customers, insurance products, etc., and no separate deployments are needed when APIs are updated as everything is 100% configured.

Implementation considerations

General considerations

TIA Services & Solutions has built up substantial know-how within taking a standard deliverable to customers and ensuring that the final solution caters to the customer-specific needs. TIA Services & Solutions' offering provides a solid plan of action and best practices on the solutions supporting POPIA.

When engaging with consultants from TIA Services & Solutions, a joint effort will identify custom code that needs to be included and potential extensions and custom forms. For the partner and the customer, this means certainty of full compliance and a working solution that is up and running with a minimum of pull on internal resources. The service will be provided with the following themes in focus:



Phase 1
Initiate and overall of data flows

Project Plan

- Agree on common perception of scope and headings
- Define project organization and clear lines of responsibilities and contacts
- Define overall timelines and deliveries
- High-level mapping of the current data flows
- Verify the current status of system documentation & authorizations
- Define overall timelines and deliveries

Phase 2
Detailed scope, and analyzing data flows

Solution Blueprint

- An detailed analysis of your current flows of data in and out of your TIA Solution
- Identify where personal data is used/stored and the relevance
- Analyzing the documenting, processes and general data flows
- How does your current handling of data comply with new rules?
- Scoping the customization needed comparing with the TIA Compliance Package
- Evaluation the effort needed to modify the TIA Compliance Package to you and the relevant TIA version

Phase 3
Design, schedule, and implement

Production Ready Solution

- Designing how the TIA Compliance Package complement your situation using the deliveries from phase 1
- Documenting/updating potential changes to current processes
- Implementing and customizing the Compliance Package from TIA
- QA'ing the overall implemented package
- Updating and documenting the data flows in scope

Retiring personal information

The TIA POPIA Compliance Package handles information stored in the standard TIA Solution. For custom solution implementation, which TIA Services & Solutions can assist with, it must be considered whether some insurance company data is outside of the TIA solution and related to the data to be deleted. Insurance companies must consider:

- Defining additional retention rules
- Customisation within the TIA solution
- Surrounding solutions like Data Warehouse (DWH), Document Management Systems, and CRM

The TIA POPIA Compliance Package provides tools that make it possible to trigger deletion of dependant data in non-TIA Solution sources. TIA Technology can help set up specific rules and integrations to other solutions to trigger data deletion.

Access limitations

The solution is utilising the existing authorisation functionality within TIA, hence, implementation will require that you revisit configuration of roles, profiles and authorisations as well as configuration of "special personal information". TIA Services & Solutions assists you in categorising data and ensuring the appropriate protection.

Monitoring user activities

The support for this requirement is covered by many initiatives, for example defining an incident plan of actions. TIA Services & Solutions assists with best practice on tracking or auditing of queried data[3], as well as configuring handling of incidents and automatic identification or privation of incidents.

Customer participations

TIA is delivering a generic Application Programming Interface (API), which is to be tailored to local requirements and application landscape. Any local communication platform must be amended with the handling of customers requesting and delivering information, for example, when a customer portal needs a "your personal information" page.

The content of the APIs is to be configured in the TIA configuration area based on the local definition of "own" data. TIA offers support for the API and can help develop or tailor APIs optimised for local requirements.

Consent and suspension of information handling

The solution will not require configuration; the only implementation effort considered is adding a consent attribute to your TIA implementation.

[3] Utilzing Oracle standard tools: https://www.oracle.com/database/security/audit-vault-database-firewall/index.html

Summary

The below table lists the conditions for compliance discussed in this white paper and summarises the suggested solution for each.

Requirement	Solution	Implementation
Condition 1: Accountability	No direct impact on TIA installations.	N/A.
Condition 2: Processing Limitations	Enable a lock on manual handling.	Grant lock authorisation to relevant person/role, for example Information Officer.
Condition 3: Purpose specification	Delete information based on predefined rule set.	Configure rules for deletion. Address information in the entire IT landscape, which could lead to integration work between TIA and other applications.
Condition 4: Further processing Limitations	No direct impact on TIA installations.	N/A.
Condition 5: Information quality	No direct impact on TIA installations.	N/A
Condition 6: Openness	No direct impact on TIA installations.	N/A
Condition 7: Security safeguards	New authorisations on data access, e.g., authorisation on claim with a specific class or specific party data.	Revisit configuration of roles and authorisations.
	Utilise existing security and add additional logging to ensure audit trail in case of breach.	Best practices on processes, configuration of role and responsibilities. Technical support of audit on queries.
Condition 8: Data subject participation	Standard API for integration to customer portals, output solutions etc.	Evaluate data set in API and implement the communication channels e.g. portal site, report etc.

Timeline

Functionality within TIA POPIA Compliance package was released with TIA 7.5.1 in August 2017 and with TIA 6.4.4 in September 2017.

TIA Technology is currently engaging with authorities, legal advisors and customers, and is participating in knowledge groups within various interest organisations to ensure that TIA incorporates any last-minute adjustments to regulations that may come from authorities.

Simultaneously, the TIA Services & Solution team has prepared an offering of services that will ensure that you follow a structured and efficient process towards compliance. The process follows best-practices for compliance proposed by legal advisors. The services include analysing IT and data landscapes, planning the roll-out of adjustments and more. We recommend that you start your analyses and planning as soon as possible to ensure that you are ready to receive the TIA POPIA compliance package and meet compliance on time.

Please engage with your TIA Engagement Director to build a specific plan for you.

FAQs

Will the solution be ready for my version of TIA? The TIA POPIA Compliance Package is released with TIA 6.4.4 and TIA 7.5.1 (Forms and ADF). TIA implementation services can include an upgrade to the newest TIA version or enable the functionality for a specific customer implementation. This is subject to a separate service agreement.

Can and will TIA support POPIA? Yes, TIA is supporting the relevant POPIA conditions. However, it is important to evaluate the entire IT landscape and processes.

What about my custom forms?
By engaging with TIA Services & Solutions you will be able to get a customised implementation embedding your own developed code.

How do I get audit on queried/viewed data? Our interpretation is that regulation is not enforcing a log on all queried data as we are ensuring that only authorised persons can access data. However, this is an interpretation based on general dialogues with legal advisors at customers and authorities. Local interpretations could impose full audit on viewed data. This can be activated with Oracle Audit[1]. Oracle Audit enables the set-up of a logging mechanism to track and document who has access to which data in the TIA solution. TIA will deliver a standard configuration and a cookbook for activation of Oracle Audit[4]. TIA Services & Solutions can support you in the analysis and do the actual implementation of Oracle Audit.

Will anonymization or encryption of data be sufficient for Purpose Specification?
This is an ongoing discussion in the community. The essence is that you do not comply with POPIA if you can reconstruct data or if you in any way can link or trace data to a person. POPIA talks explicitly about preventing reconstruction of de-identified personal information. TIA needs to keep policy id, party id etc., to keep the database integrity. Those identifiers could potentially identify a person. Especially if correlated with other data. That will result in a POPIA breach. Hence, deletion is the only certain solution for the requirement.

The Act promotes storage of information for historical, statistical or research purposes with appropriate safeguards. TIA BI cloud ensures that data is de-identified by anonymising it without any possibilities for reconstruction. The existing security mechanism provides a safety on data access.

What is the commercial impact? The TIA POPIA Compliance Package is introducing new functionality. The right to use the new functionality is subject to separate contract. Oracle Audit is a separate Oracle solution with separate license (see above). TIA Services & Solutions offerings are consultancy services following TIA consultancy rates.

[4] https://www.oracle.com/database/security/audit-vault-database-firewall/index.html

When should I start my compliance implementation? Now. TIA recommends that you start TIA analysis phase 1 (see above) as soon as possible to meet the compliance deadline.

What's next? Your TIA Engagement Director will contact you during 2018 to start a conversation about implementing POPIA. If you have further questions, please feel free to contact Ilse Willemse, iwi@tiatechnology.com

This document may not be reproduced or transmitted in any form or by any means, for any purpose, without prior written approval of TIA Technology A/S. The contents of this document are continually subject to amendment without prior notice. Although due care and diligence has been taken to ensure accuracy of this document, TIA Technology A/S does not undertake any liability for the accuracy of the document, including errors and omissions.

This document shall not impose any obligations on TIA Technology A/S by any means.

South African office

TIA Technology
The Workplace
140a Kelvin drive
Morningside manor
Johannesburg
South Africa

T +27 11 064 1677

iwi@tiatechnology.com
www.tiatechnology.com

Closer to Customers